======= WPI =======

TI - Encryption and authentication system for use in providing communication security in communication network

AB - JP2000004223 NOVELTY - The encryption sentence of a communication device is decoded by an encryption decoder (19) to obtain an n-bit encryption key. A dummy random-number series is obtained to input the n-bit encryption key in a dummy random-number generator (21). A decoding device (19) obtains a communication signal by performing OR operation of dummy random-number series and encryption sentence of the communication device.

- DETAILED DESCRIPTION - The disclosure key encryption device (11) of an encryption apparatus (7) produces a predetermined encryption key by performing the encryption of another encryption key with the disclosure key, based on a public-key crypto system. A dummy random-number series is obtained to input the output value of the bits of an n-step linear feedback shift register into a bent function, and to input the n-bit encryption key of the communication signal into the dummy random-number generator. The encryption apparatus obtains the encryption sentence by applying the exclusive OR operation to the dummy random-number series and communication signal. The communication device performs the communication of the encryption key and the encryption sentence.
- USE - For use in providing communication security in communication network.
- ADVANTAGE - Improves safety of data communication in communication network. Ensures high-speed encryption and authentication system.
- DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of an encryption and authentication system.
- Encryption apparatus 7
- Disclosure key encryption device 11
- Decoding device 19
- Encryption decoder 19
- Dummy random-number generator 21
- (Dwg.1/4)

PN - JP2000004223 A 20000107 DW200012 H04L9/26 007pp
PR - JP19980185610 19980616
PA - (TOCM) TOYO COMMUNICATION EQUIP CO
MC - W01-A05A W01-A05B
DC - P85 W01
IC - G09C1/00 ;H04L9/26 ;H04L9/32
AN - 2000-132818 [12]

======= PAJ =======

TI - ENCRYPTION/AUTHENTICATION SYSTEM

AB - PROBLEM TO BE SOLVED: To provide an encryption/authentication system which is immune to various attack methods and which uses a high-speed pseudo random number generator.

- SOLUTION: Concerning this enciphery/authentication system, a cryptographic key KA is enciphered by a public key, an enciphered key KeyA is generated, the output value of (n) bits from an n-step linear feedback shift register is inputted to a Bent function 13, a pseudo random number sequence is obtained by inputting the enciphered key KA of (n) bits to the seed of the pseudo random number generator for obtaining the output of 1 bit, an enciphered sentence CryptoA is obtained by performing exclusive ORing operation 15 with the plain sentence, and the key KeyA and enciphered sentence CryptoA are communicated. Then the enciphered sentence CryptoA is deciphered by the secret key and the enciphered key KA of (n) bits is obtained. The enciphered key KA is inputted to the seed of the pseudo random number generator, the pseudo random number sequence is obtained and the plain sentence is obtained by exclusive ORing operation 23 with the enciphered sentence CryptoA.

PN - JP2000004223 A 20000107
PD - 2000-01-07
ABD - 20000831
ABV - 200004
AP - JP19980185610 19980616
PA - TOYO COMMUN EQUIP CO LTD
IN - SUGIMOTO KOICHI
I - H04L9/26 ;G09C1/00 ;H04L9/32

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－4223
（P2000－4223A）
(43)公開日　平成12年１月７日(2000.1.7)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	9/26		Ｈ０４Ｌ	9/00	６５９	５Ｋ０１３
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｄ	
		６４０			６４０Ａ	
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ａ	

審査請求　未請求　請求項の数３　ＦＤ　（全７頁）

(21)出願番号　特願平10－185610

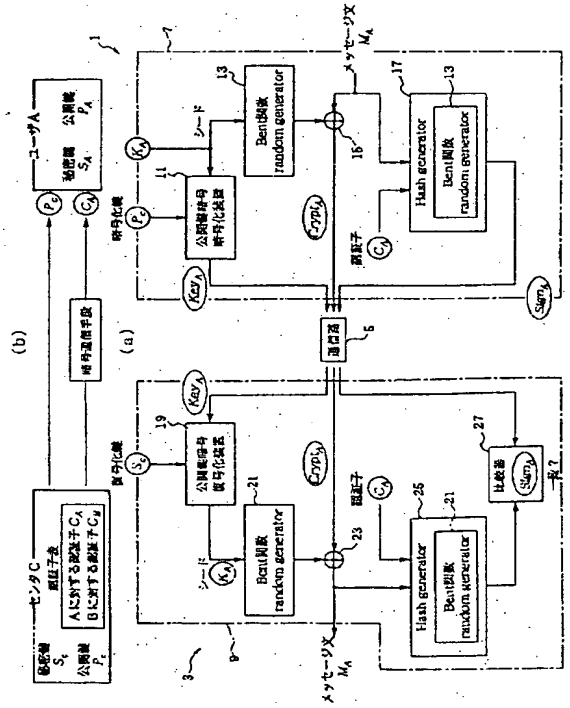
(22)出願日　平成10年６月16日(1998.6.16)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　杉本　浩一
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内
(74)代理人　100085660
弁理士　鈴木　均

Ｆターム(参考)　5K013 CA00 CA04 CA17 FA07 GA05

(54)【発明の名称】　暗号・認証システム

(57)【要約】　（修正有）
【課題】　種々の攻撃法に対して強固で、かつ高速な疑似乱数生成器を用いた暗号・認証システムを提供する。
【解決手段】　暗号化鍵K_Aを公開鍵で暗号化して暗号化された鍵Key_Aを生成する。ｎ段線形フィードバックシフトレジスタのｎビットの出力値をＢｅｎｔ関数１３に入力し、１ビットの出力を得る疑似乱数生成器のシードに平文のｎビットの暗号化鍵K_Aを入力して疑似乱数系列を得、平文と排他的論理和演算１５をして暗号文$Crypto_A$を得、鍵Key_A、暗号文$Crypto_A$を通信する。暗号文$Crypto_A$を秘密鍵で復号化し、ｎビットの暗号化鍵K_Aを得る。暗号化鍵K_Aを疑似乱数生成器のシードに入力して疑似乱数系列を得、暗号文$Crypto_A$と排他的論理和演算２３で平文を得る。



【特許請求の範囲】

【請求項1】 平文を暗号化して通信し、その暗号化された平文を復号するための暗号システムであって、

暗号化鍵K_Aを公開鍵で暗号化して暗号化された鍵Key_Aを生成する公開鍵暗号方式に基づく公開鍵暗号暗号化装置と、

n段線形フィードバックシフトレジスタのnビットの出力値をBent関数に入力し、1ビットの出力を得る疑似乱数生成器のシードに上記平文のnビットの暗号化鍵K_Aを入力することで疑似乱数系列を得、その疑似乱数系列と平文とに排他的論理和演算を施すことで暗号文$Crypto_A$を得る暗号化装置と、

上記鍵Key_A、暗号文$Crypto_A$を通信するための通信手段と、

上記通信手段よりの暗号文$Crypto_A$を秘密鍵で復号化し、nビットの暗号化鍵K_Aを得る公開鍵暗号方式に基づく公開鍵暗号復号化装置と、

上記通信手段よりの暗号化鍵K_Aを上記疑似乱数生成器のシードに入力することで疑似乱数系列を得、その疑似乱数系列と上記通信手段よりの暗号文$Crypto_A$とに排他的論理和演算を施すことで上記平文を得る復号化装置とを有することを特徴とする暗号システム。

【請求項2】 上記疑似乱数生成器に用いられるBent関数が、mビットの数x_1、x_2を用い、mビット入力1ビット出力の論理関数をgとし、mビット入力mビット出力の全単射論理関数をπとした場合、$f(x_1, x_2) = \pi(x_1) \cdot x_2 + g(x_1)$と表されることを特徴とする請求項1に記載の暗号システム。

【請求項3】 平文を暗号化して通信し、その暗号化された平文を復号すると共に認証を行うための暗号・認証システムであって、

暗号化鍵K_Aを公開鍵で暗号化して暗号化された鍵Key_Aを生成する公開鍵暗号方式に基づく公開鍵暗号暗号化装置と、

n段線形フィードバックシフトレジスタのnビットの出力値をBent関数に入力し、1ビットの出力を得る疑似乱数生成器のシードに上記平文のnビットの暗号化鍵K_Aを入力することで疑似乱数系列を得、その疑似乱数系列と平文とに排他的論理和演算を施すことで暗号文$Crypto_A$を得る暗号化装置と、

認証子および上記平文を上記疑似乱数生成器に入力することで、改ざん検出および認証のためのハッシュ値$Sign_A$を得るデジタル署名装置と、

上記鍵Key_A、暗号文$Crypto_A$、およびハッシュ値$Sign_A$を通信するための通信手段と、

上記通信手段よりの暗号文$Crypto_A$を秘密鍵で復号化し、nビットの暗号化鍵K_Aを得る公開鍵暗号方式に基づく公開鍵暗号復号化装置と、

上記通信手段よりの暗号化鍵K_Aを上記疑似乱数生成器のシードに入力することで疑似乱数系列を得、その疑似乱数系列と上記通信手段よりの暗号化$Crypto_A$とに排他的論理和演算を施すことで平文を得る復号化装置と、

上記得られた平文と認証子を上記疑似乱数生成器に入力することで、ハッシュ値$Sign'_A$を得、入力されたハッシュ値$Sign_A$と比較し、一致していれば得られた平文が改ざんされていなく正当な相手から送られたものであると判定するデジタル認証装置とを有することを特徴とする暗号・認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機密の保証されない通信網における通信の機密保護をはかると共に、通信文の改ざんの有無および通信相手の正当性を確認するための暗号・認証システムに関し、特に、種々の攻撃法に対して強固で、かつ高速な疑似乱数生成器を用いた暗号・認証システムに関する。

【0002】

【従来の技術】現在、暗号は大別して秘密鍵暗号と公開鍵暗号の2種類が存在する。秘密鍵暗号というのは、暗号化と復号に同じ鍵を用いる暗号化手法である。これは、「慣用暗号」あるいは「対称鍵暗号」とも呼ばれる。一方、公開鍵暗号とは、暗号化と復号に異なる鍵を用いる手法である。上記秘密鍵暗号は、暗号化と復号の鍵が同一であるので、鍵を共有するための手段が必要になるが、高速に暗号化および復号が行えるという性質を持つ。一方、上記公開鍵暗号は暗号化の鍵と復号のための鍵が異なるので、暗号化の鍵を機密の保証されない通信網で配送することが可能であるが、暗号化および復号が低速であるという性質を持つ。このため、高速な暗号システムを構成する場合、一般に、暗号化および復号は秘密鍵暗号を用い、その鍵を公開鍵暗号によって暗号化し、配送するという方法を用いている。この方式を採用しているものには、PGP、PEM等がある。上記秘密鍵暗号の中にはブロック暗号とストリーム暗号が存在する。ブロック暗号は、図4（a）に示す様に平文を一定のブロック毎に区切り、そのブロック毎に同じ鍵で暗号化を行うものである。一方、ストリーム暗号は、図4（b）に示す様に1文字または1ビット毎に異なる鍵で他の文字やビットに変換するものである。上記ブロック暗号、ストリーム暗号については、電気通信学会「現代暗号理論」等に記載されている。上記ストリーム暗号の中には情報理論的に解読が不可能とされているバーナム暗号が存在する。バーナム暗号は平文と同じビット長の無限周期の乱数列を1回限りの使い捨て鍵（one－time－pad）として用い、平文とビット毎に排他的論理和をとることで暗号文を得る。

【0003】しかし、鍵長が平文の長さと同じことは、暗号システムを構成する上で非現実的であり、一般的には疑似乱数生成器によって生成された疑似乱数をone

－ｔｉｍｅ－ｐａｄの代わりとして用い、そのシードを暗号化鍵とするのが普通である。この疑似乱数生成器には、生成された疑似乱数列から次の疑似乱数列の推定が困難であるという性質が要求される。上記疑似乱数生成器には、（１）線形フィードバックシフトレジスタ、（２）非線形フィードバックシフトレジスタ、（３）線形フィードバックシフトレジスタを用いたＦｉｌｔｅｒ　Ｇｅｎｅｒａｔｏｒ、（４）非線形フィードバックシフトレジスタを用いたＦｉｌｔｅｒ　Ｇｅｎｅｒａｔｏｒ、（５）非線形コンバイナ、（６）計算量的安全疑似乱数等があり、実用的には（１）～（５）があげられる。この中で、（１）、（２）には構造を公開した場合においてそのレジスタの段数分の連続する出力を知ることにより、系列が容易に推定できるという問題点がある。上記の生成された疑似乱数列から次の疑似乱数列を推定する方法は疑似乱数生成器に対する攻撃法と呼ばれる。上記疑似乱数生成器に対する攻撃法としては、主として以下の方法がある。

（ａ）非線形関数の線形近似を利用して、出力から入力の線形フィードバックレジスタのある時刻における状態を推定し、それ以後のレジスタの値を決定する。（Ｃｏｒｒｅｌａｔｉｏｎ　Ａｔａｃｋ）

（ｂ）バーレカンプ＝マッシーのアルゴリズムを利用して等価な線形フィードバックシフトレジスタを構成する。

（ｃ）初期値の全数検索。

（ｄ）以上の組み合わせ。

暗号用として採用可能な疑似乱数生成器は、上記の（ａ）～（ｄ）の攻撃法に対して強固である必要がある。

【０００４】

【発明が解決しようとする課題】しかしながら、従来の疑似乱数生成器では、上記（ａ）～（ｄ）の攻撃に対しての強度を高めると、疑似乱数を得るための計算が複雑になって演算速度が遅くなり、演算速度を速くすると上記（ａ）～（ｄ）の攻撃に対する強度が下がるという性質があり、これを用いた暗号／認証システムも、同様の性質を有してしまうという欠点があった。本発明は、上記事情に鑑みてなされたものであって、種々の攻撃法に対して強固で、かつ高速な疑似乱数生成器を用いた暗号・認証システムを提供することである。

【０００５】

【課題を解決するための手段】上記目的を達成するため、本発明は、平文を暗号化して通信し、その暗号化された平文を復号するための暗号システムにおいて、暗号化鍵K_Aを公開鍵で暗号化して暗号化された鍵Key_Aを生成する公開鍵暗号方式に基づく公開鍵暗号暗号化装置と、ｎ段線形フィードバックシフトレジスタのｎビットの出力値をＢｅｎｔ関数に入力し、１ビットの出力を得る疑似乱数生成器のシードに上記平文のｎビットの暗号化鍵K_Aを入力することで疑似乱数系列を得、その疑似乱数系列と平文とに排他的論理和演算を施すことで暗号文$Crypto_A$を得る暗号化装置と、上記鍵Key_A、暗号文$Crypto_A$を通信するための通信手段と、上記通信手段よりの暗号文$Crypto_A$を秘密鍵で復号化し、ｎビットの暗号化鍵K_Aを得る公開鍵暗号方式に基づく公開鍵暗号復号化装置と、上記通信手段よりの暗号化鍵K_Aを上記疑似乱数生成器のシードに入力することで疑似乱数系列を得、その疑似乱数系列と上記通信手段よりの暗号文$Crypto_A$とに排他的論理和演算を施すことで上記平文を得る復号化装置とを有することを特徴とする。本発明の他の特徴は、上記疑似乱数生成器に用いられるＢｅｎｔ関数が、ｍビットの数x_1、x_2を用い、ｍビット入力１ビット出力の論理関数をｇとし、ｍビット入力ｍビット出力の全単射論理関数をπとした場合、$f(x_1, x_2) = \pi(x_1) \cdot x_2 + g(x_1)$と表されることである。本発明の他の特徴は、平文を暗号化して通信し、その暗号化された平文を復号すると共に認証を行うための暗号・認証システムにおいて、暗号化鍵K_Aを公開鍵で暗号化して暗号化された鍵Key_Aを生成する公開鍵暗号方式に基づく公開鍵暗号暗号化装置と、ｎ段線形フィードバックシフトレジスタのｎビットの出力値をＢｅｎｔ関数に入力し、１ビットの出力を得る疑似乱数生成器のシードに上記平文のｎビットの暗号化鍵K_Aを入力することで疑似乱数系列を得、その疑似乱数系列と平文とに排他的論理和演算を施すことで暗号文$Crypto_A$を得る暗号化装置と、認証子および上記平文を上記疑似乱数生成器に入力することで、改ざん検出および認証のためのハッシュ値$Sign_A$を得るデジタル署名装置と、上記鍵Key_A、暗号文$Crypto_A$、およびハッシュ値$Sign_A$を通信するための通信手段と、上記通信手段よりの暗号文$Crypto_A$を秘密鍵で復号化し、ｎビットの暗号化鍵K_Aを得る公開鍵暗号方式に基づく公開鍵暗号復号化装置と、上記通信手段よりの暗号化鍵K_Aを上記疑似乱数生成器のシードに入力することで疑似乱数系列を得、その疑似乱数系列と上記通信手段よりの暗号化$Crypto_A$とに排他的論理和演算を施すことで平文を得る復号化装置と、上記得られた平文と認証子を上記疑似乱数生成器に入力することで、ハッシュ値$Sign'_A$を得、入力されたハッシュ値$Sign_A$と比較し、一致していれば得られた平文が改ざんされていなく正当な相手から送られたものであると判定するデジタル認証装置とを有することである。

【０００６】

【発明の実施の形態】本発明を図示した実施形態に基づいて説明する。図１は、本発明による暗号・認証システムの一実施形態を示す構成図である。図１（ａ）に示す様に、この暗号・認証システムは、ユーザＡの端末１からセンタＣの装置３へ通信路５を介して情報（暗号化さ

れたメッセージ文等）を送り、上記装置３で復号すると共に認証も行うものであり、そのために、上記端末１は暗号装置７を有し、上記センタＣの装置３は復号装置９を有している。上記暗号装置７は、鍵K_A および暗号化鍵P_C が入力されると共に上記通信路５に接続された公開鍵暗号暗号化装置１１と、上記鍵K_A が入力される第１の疑似乱数生成器１３と、メッセージ文M_A が入力されると共に上記第１の疑似乱数生成器１３および上記通信路５に接続された第１の排他的論理和演算器１５と、上記メッセージ文M_A および認証子C_A が入力されると共に上記通信路５に接続された第１のハッシュ値生成器１７とを有している。ここで、上記第１のハッシュ値生成器１７に用いられる疑似乱数生成器は、上記第１の疑似乱数生成器１３と兼用されている。

【０００７】次に、上記復号装置９は、復号化鍵S_C が入力されると共に上記通信路５に接続された公開鍵暗号復号化装置１９と、上記公開鍵暗号復号化装置１９に接続された第２の疑似乱数生成器２１と、上記第２の疑似乱数生成器２１および通信路５に接続された第２の排他的論理和演算器２３と、認証子C_A が入力されると共に上記第２の排他的論理和演算器２３に接続された第２のハッシュ値生成器２５と、上記第２のハッシュ値生成器２５と通信路５と間に接続された比較器２７とを有している。ここで、上記第２のハッシュ値生成器２５に用いられる疑似乱数生成器は、上記第２の疑似乱数生成器２１と兼用されている。そして、本発明では、上記第１および第２の疑似乱数生成器１３、２１がＢｅｎｔ関数を用いた疑似乱数生成器となっている。

【０００８】以下、このＢｅｎｔ関数を用いた疑似乱数生成器１３、２１について説明する。上記第１および第２の疑似乱数生成器１３、２１にＢｅｎｔ関数を用いるに当って、図２に示すような線形フィールドバックシフトレジスタを用いたＦｉｌｔｅｒ Ｇｅｎｅｒａｔｏｒ形の疑似乱数生成器を考え、この関数部Ａに対して前述した種々の攻撃法に最も強い関数として、Ｂｅｎｔ関数を用いている。そして、論理関数のＢｅｎｔ関数は、ｍビット入力１ビット出力の論理関数ｇ、ｍビット入力ｍビット出力の全単射論理関数π、ｍビットの数x_1 、x_2 を用いて、$f(x_1, x_2) = \pi(x_1) \cdot x_2 + g(x_1)$ と表される。また、この関数を上記攻撃法に対して、強度を増やすために、最大の非線形性を少々犠牲にして関数ｇを２ｍビット入力１ビット出力としている。この場合の関数は、$f(x_1, x_2) = \pi(x_1) \cdot x_2 + g(x_1, x_2)$ となる。

【０００９】上記図２に示した関数部Ａの概略構成を示すと図３に示す様になる。すなわち、図３に示す様に、２ｍ段線形フィードバックシフトレジスタ２９に接続されたｇ関数演算部３１と、上記２ｍ段線形フィードバックシフトレジスタ２９に接続されたπ関数演算部３３と、上記π関数演算部３３と２ｍ段線形フィードバックシフトレジスタ２９との間に接続された乗算器３５と、上記ｇ関数演算部３１と乗算器３５との間に接続された排他的論理和演算器３７とを有している。従って、上記２ｍ段線形フィードバックシフトレジスタ２９よりのｍビットの数x_1 、x_2 は、上記ｇ関数演算部３１、π関数演算部３３、乗算器３５、および排他的論理和演算器３７を通して$f(x_1, x_2) = \pi(x_1) \cdot x_2 + g(x_1, x_2)$ で表わされる疑似乱数列となって出力される。なお、Ｂｅｎｔ関数については、”Ｃｏｎｔｅｍｐｏｒａｒｙ Ｃｒｙｐｔｏｌｏｇｙ”：Ｔｈｅ Ｓｃｉｅｎｃｅ ｏｆ Ｉｎｆｏｒｍａｔｉｏｎ Ｉｎｔｅｇｒｉｔｙ，Ｇ．Ｓｉｍｍｏｎｓ，ｅｄ．，ＩＥＥＥｐｒｅｓｓに、Ｂｅｎｔ関数を２．２の攻撃法に対してより強度にする方法、これを用いた疑似乱数生成装置の高速性については、杉田誠「Ｂｅｎｔ関数を用いた暗号／認証用疑似乱数生成法」電子通信学会技術研究報告、ＩＳＥＣ９５－１４ Ｊｕｌｙ，１９９５に記載されている。

【００１０】次に、上記図１（ａ）に示した暗号・認証システムの動作について説明する。まず、通常動作の前に、図１（ｂ）に示す様に、センターＣは各々のそれぞれのユーザに対してそれぞれ異なる認証子C_A 、C_B 、…を発行し、ＥＩＧａｍａｌ暗号方式のような公開鍵暗号通信手段により、その認証子を配送しておく。次に、図１（ａ）に示す様に、上記ユーザＡがセンターＣに対して暗号通信を行うときは、ユーザＡはメッセージ文M_A を暗号化する鍵K_A を上記公開鍵暗号暗号化装置１１によってセンターＣの公開する公開鍵P_C で暗号化し、暗号化鍵Key_A を生成する。また、上記鍵K_A をＢｅｎｔ関数を用いた第１の疑似乱数生成器１３のシードとして疑似乱数列を生成し、それとメッセージ文M_A に第１の排他的論理和演算器１５により排他的論理和演算を施すことにより、暗号文$Crypt_A$ を得る。さらに、上記センターＣがユーザＡに対して発行した認証C_A とメッセージ文M_A を上記第１の疑似乱数生成器１３からなる第１のハッシュ値生成器１７を用いることにより、ハッシュ値$Sign_A$ をデジタル署名として生成する。そして、上記ユーザＡはセンターＣに生成した３つ組（Key_A 、$Crypt_A$ 、$Sign_A$ ）を上記通信路５を介して送信する。

【００１１】次に、上記センターＣがユーザＡからのメッセージ文を復号し、その妥当性を検証するやり方は、以下のように行う。まず、上記ユーザＡから受信した（暗号化鍵Key_A 、暗号文$Crypt_A$ 、ハッシュ値$Sign_A$ ）のうちの暗号化鍵Key_A を上記センターＣの秘密鍵S_C で復号化し、鍵K_A を得る。次に、上記鍵K_A をＢｅｎｔ関数を用いた第２の疑似乱数生成器２１のシードとして疑似乱数列を生成し、それと暗号文$Crypt_A$ とを第２の排他的論理和演算器２３により排他的論理和演算を施すことにより、メッセージ文M_A を

復元する。さらに、上記認証子C_Aと復元されたメッセージ文M_Aを上記第２の疑似乱数生成器２１に入力することで、ハッシュ値$Sign_A'$を得、これを受信したハッシュ値$Sign_A$と比較器２７で比較し、一致していれば、復元されたメッセージ文M_Aが正当なものとみなす。ここで、上記認証子C_AはユーザＡとセンターＣのみしか知らないので、センターＣはメッセージ文M_AがユーザＡから送られたものであると判断し、また、復元されたメッセージ文M_Aが改ざんされたものであれば、それから計算された$Sign_A'$と受信した$Sign_A$は一致しない。上記センターＣがユーザＡに対して平文を送信するときも同様な手順で行う。すなわち、センターＣとユーザＡが認証の必要のない通信を行う場合、認証子C_Aの代用として鍵K_Aを用いることができる。この場合、メッセージ文M_Aの改ざんを検出することが可能である。また、ユーザＡとユーザＢが通信を行う場合もこれと同様な手順となる。

【００１２】

【発明の効果】本発明は、以上説明したように、暗号、認証部にＢｅｎｔ関数を用いた疑似乱数生成器を採用することにより、安全性が高く、かつ、高速な暗号・認証システムを作成することができる。また、暗号部、認証部の両方にＢｅｎｔ関数を用いた疑似乱数生成器を採用することで、このシステムの強度は、公開鍵暗号部を除いて、Ｂｅｎｔ関数の一方向性にのみ依存させることができる。

【図面の簡単な説明】

【図１】（ａ）および（ｂ）は本発明による暗号・認証システムの一実施形態を示す構成図である。

【図２】図１に示したＢｅｎｔ関数を利用した疑似乱数生成器の概念図である。

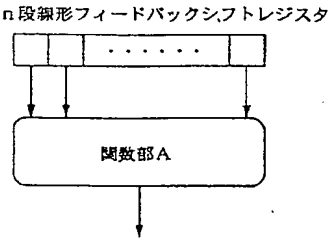
【図３】図１に示したＢｅｎｔ関数を利用した疑似乱数生成器の概念図である。

【図４】（ａ）および（ｂ）は従来の暗号生成方法の内のストリーム方式およびブロック方式を示す説明図である。

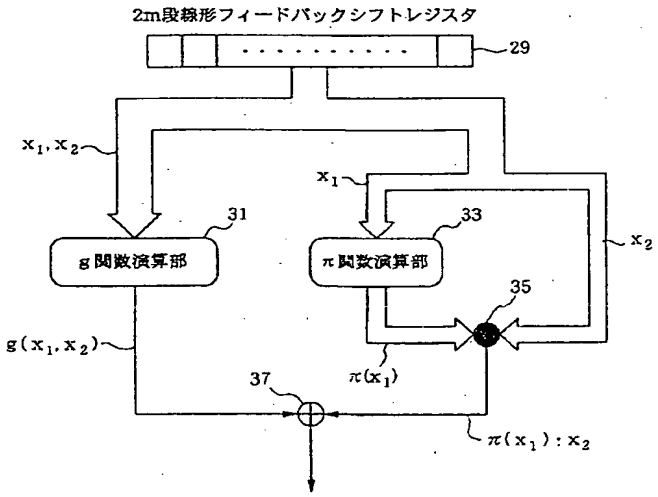
【符号の説明】

１…端末、　３…装置、５…通信路、　７…暗号装置、９…復号装置、１１…公開鍵暗号暗号化装置、１９…公開鍵暗号復号化装置、１３、２１…疑似乱数生成器、１５、２３、３７…排他的論理和演算器、１７、２５…ハッシュ値生成器、　２７…比較器、２９…２ｍ段線形フィードバックシフトレジスタ、３１…ｇ関数演算部、　３３…π関数演算部、３５…乗算器、

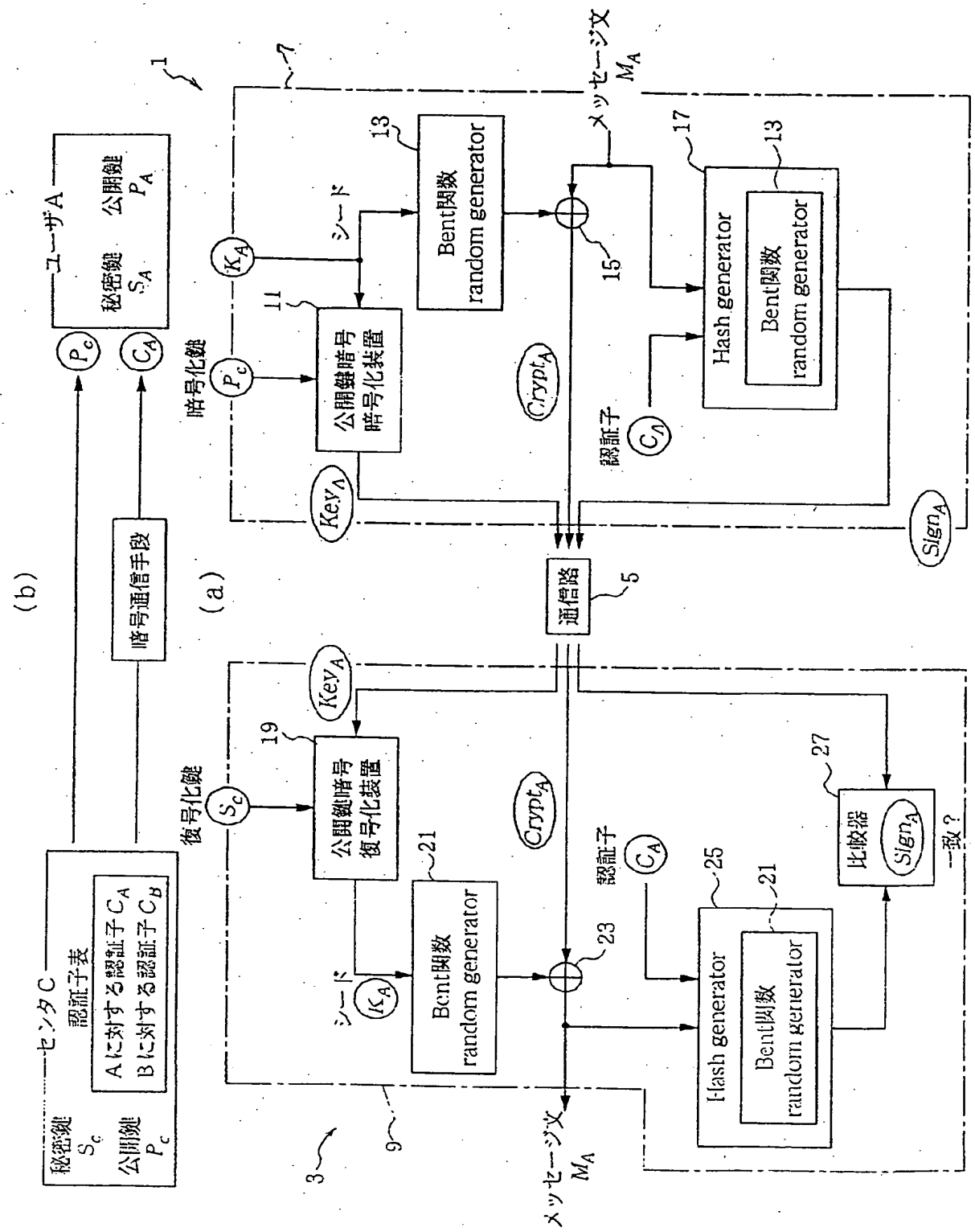
【図２】



【図３】



【図1】


(b)
(a)
ユーザA
秘密鍵 S_A
公開鍵 P_A
センタC
認証子表
Aに対する認証子 C_A
Bに対する認証子 C_B
秘密鍵 S_c
公開鍵 P_c
暗号通信手段
暗号化鍵
復号化鍵
公開鍵暗号装置
公開鍵暗号復号化装置
シード
Bent関数 random generator
Hash generator
Bent関数 random generator
認証子
比較器
一致？
通信路
メッセージ文 M_A
Key_A
$Crypt_A$
$Sign_A$
K_A
C_A
1
3
5
7
9
11
13
15
17
19
21
23
25
27

【図4】